

INTERFERENCE SEARCH

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L3	1	(system action electronic communication identity public key database sender encode\$3).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/03/27 17:04
L4	1	(system action electronic communication identity public key database association encode\$3).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/03/27 17:03
L13	1	(sender identity information public key account association electronic communication private receiver computer database step encod\$3).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/03/27 17:08
L15	1	(sender identity information public key account association electronic communication private receiver step encod\$3).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/03/27 17:09
L16	1	(sender identity information public key account association electronic communication private step encod\$3).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/03/27 17:09
L17	1	(sender identity information public key account association electronic communication private encod\$3).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/03/27 17:09
L18	2	(identity information public key account association electronic communication private encod\$3).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/03/27 17:09
L19	2	(identity information public key account association electronic private encod\$3).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/03/27 17:09
L20	2	(identity public key account association electronic private encod\$3).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/03/27 17:10

EAST Search History

L21	2	(identity public key account association electronic private predetermin\$3).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/03/27 17:10
-----	---	---	--	-----	----	------------------

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	5834	((380/255) or (713/176) or (713/181) or (716/156) or (713/175) or (713/182) or (705/57) or (705/64)).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/27 18:25
L2	859	L1 and @ad<"19980911"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/27 17:48
L3	99	L1 and encod\$3 and compar\$3 and "public key" and "private key" and authenticat\$3 and account and sender and communication and identity and predetermin\$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/27 17:56
L4	11	L2 and L3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/27 17:59
L6	681	encod\$3 and compar\$3 and "public key" and "private key" and authenticat\$3 and message and account and sender and communication and identity and predetermin\$3 and associat\$3 and validat\$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/27 18:01
L7	9	L6 and L2	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/27 18:02
L8	8045	wheeler.inv.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/27 18:02
L11	59	L8 and lynn and anne	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/27 18:25
L12	65	public same private same key same pair same associat\$3 same account same database	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/27 18:26

EAST Search History

L14	20	L12 and identity and encod\$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/27 18:27
L15	0	L14 and @ad<"19981109"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/27 18:27



[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

Search: ☒ The ACM Digital Library ☐ The Guide

encod\$3 and compar\$3 and "public key" and "private key" and



THE ACM DIGITAL LIBRARY

[Feedback](#) [Report a problem](#) [Satisfaction s](#)

Terms used encod\$3 and compar\$3 and public key and private key and authenticat\$3 and message and account and sender and communication and identity and predetermi

Sort results by

[Save results to a Binder](#)

Try an [Advanced Search](#)

Display results

[Search Tips](#)

Try this search in [The ACM Gui](#)

☐ Open results in a new window

Results 1 - 20 of 200

Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

Best 200 shown

Relevance scal

1 [Communication privacy: Secure off-the-record messaging](#)



Mario Di Raimondo, Rosario Gennaro, Hugo Krawczyk

November 2005 **Proceedings of the 2005 ACM workshop on Privacy in the electronic society '05**

Publisher: ACM Press

Full text available: pdf(181.59 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

At the 2004 Workshop on Privacy in the Electronic Society (WPES), Borisov, Goldberg and Brew presented "Off the Record Messaging" (OTR), a protocol designed to add end-to-end security ar privacy to Instant Messaging protocols. An open-source implementation of OTR is available and achieved considerable success. In this paper we present a security analysis of OTR showing that the overall concept of the system is valid and attractive, the protocol suffers from security shortcomings du ...

Keywords: authentication, deniability, instant messaging, perfect forward secrecy

2 [Privacy/anonymity: Receiver anonymity via incomparable public keys](#)



Brent R. Waters, Edward W. Felten, Amit Sahai

October 2003 **Proceedings of the 10th ACM conference on Computer and communications security CCS '03**

Publisher: ACM Press

Full text available: pdf(230.49 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index term](#)

We describe a new method for protecting the anonymity of message receivers in an untrusted network. Surprisingly, existing methods fail to provide the required level of anonymity for receiv (although those methods do protect sender anonymity). Our method relies on the use of multic along with a novel cryptographic primitive that we call an Incomparable Public Key cryptosyster which allows a receiver to efficiently create many anonymous "identities" for itself without divul that these ...

Keywords: PGP, anonymity, privacy, public key cryptography

3 [Trust, recommendations, evidence, and other collaboration know-how \(TRECK\): Strong pseudonymous communication for peer-to-peer reputation systems](#)



Michael Kinateder, Ralf Terdic, Kurt Rothermel

March 2005 **Proceedings of the 2005 ACM symposium on Applied computing SAC '05**

Publisher: ACM Press

Full text available:  [pdf\(231.59 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#), [review](#)

In this paper we present a novel approach to enable untraceable communication between pseudonyms. Our work provides strong sender and recipient anonymity by eliminating the need know of each other's address. We use a variation of Chaum mixes to achieve unlinkability between sender and recipient and introduce a concept called *extended destination routing* (EDR) which r-routing headers constructed in multiple layers of encryption and published in a *distributed hash* (DH ...


Keywords: data protection, distributed reputation systems, extended destination routing, mixe pseudonymous communication

4 Secure communications between bandwidth brokers



Bu-Sung Lee, Wing-Keong Woo, Chai-Kiat Yeo, Teck-Meng Lim, Bee-Hwa Lim, Yuxiong He, Jie Son-
January 2004 **ACM SIGOPS Operating Systems Review**, Volume 38 Issue 1

Publisher: ACM Press

Full text available:  [pdf\(922.33 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#)

In the Differentiated Services (DiffServ) architecture, each domain has a Bandwidth Broker to p the resources management, primarily bandwidth reservation. In a multi-domain environment, S Inter-domain Bandwidth Broker Signaling (SIBBS) protocol is proposed for the inter-domain communication protocol proposed for bandwidth broker communication. Since the information exchanged between BBs are sensitive in sense of Service Level Agreement (SLA), the communi between the inter-domai ...

Keywords: Bandwidth Broker, Public Key Infrastructure, Simple Inter-domain Bandwidth Broke Signaling


5 New basic technologies for DIM: Pseudonym management using mediated identity-based cryptography



Thibault Candebat, Cameron Ross Dunne, David T. Gray

November 2005 **Proceedings of the 2005 workshop on Digital identity management DIM '05**

Publisher: ACM Press

Full text available:  [pdf\(293.16 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Mobile Location-Based Services (LBS) have raised privacy concerns amongst mobile phone user may need to supply their identity and location information to untrustworthy third parties in orde access these applications. Widespread acceptance of such services may therefore depend on ho privacy sensitive information will be handled in order to restore users' confidence in what could become the "killer app" of 3G networks. In this paper, we present a proxy-based public key infrastructure tha ...

Keywords: SEM architecture, identity-based encryption, location-based services, pseudonymity

6 Oblivious signature-based envelope



Ninghui Li, Wenliang Du, Dan Boneh

July 2003 **Proceedings of the twenty-second annual symposium on Principles of distribui computing PODC '03**

Publisher: ACM Press

Full text available:  [pdf\(874.99 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [citing](#)s, [index term](#)

Exchange of digitally signed certificates is often used to establish mutual trust between stranger wish to share resources or to conduct business transactions. Automated Trust Negotiation (ATN

approach to regulate the flow of sensitive information during such an exchange. Previous work are based on access control techniques, and cannot handle cyclic policy interdependency satisfactorily. We show that the problem can be modelled as a 2-party secure function evaluation (SFE) problem.

7 Wireless sensor networks: An efficient broadcast authentication scheme in wireless sensor networks



Shang-Ming Chang, Shihpyng Shieh, Warren W. Lin, Chih-Ming Hsieh

March 2006 **Proceedings of the 2006 ACM Symposium on Information, computer and communications security ASIACCS '06**

Publisher: ACM Press

Full text available: pdf(2.17 MB)

Additional Information: [full citation](#), [abstract](#), [references](#)

A broadcast authentication mechanism is important in wireless sensor networks, assuring receipt of a packet's validity. To provide authentication, some researchers utilize one way key chains and delayed disclosure of keys; however, such an approach requires time synchronization and delay authentication. Another technique uses one-time signature schemes. Unfortunately, such schemes suffer from large key sizes and a limited number of uses per key. To cope with these problems, we propose an efficient scheme.

Keywords: authentication, broadcast, key renewal, one time signature, wireless sensor network

8 Cryptography: Direct chosen ciphertext security from identity-based techniques



Xavier Boyen, Qixiang Mei, Brent Waters

November 2005 **Proceedings of the 12th ACM conference on Computer and communications security CCS '05**

Publisher: ACM Press

Full text available: pdf(305.35 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index term](#)

We describe a new encryption technique that is secure in the standard model against chosen ciphertext attacks. We base our method on two very efficient Identity-Based Encryption (IBE) schemes with random oracles due to Boneh and Boyen, and Waters. Unlike previous CCA2-secure cryptosystems that use IBE as a black box, our approach is very simple and compact. It makes direct use of the underlying IBE structure, and requires no cryptographic primitive other than the IBE scheme itself. This conveys the security of the encryption.

Keywords: chosen ciphertext security, identity-based encryption

9 The design and implementation of a private message service for mobile computers

David A. Cooper, Kenneth P. Birman

August 1995 **Wireless Networks**, Volume 1 Issue 3

Publisher: Kluwer Academic Publishers

Full text available: pdf(1.35 MB)

Additional Information: [full citation](#), [abstract](#), [references](#)

Even as wireless networks create the potential for access to information from mobile platforms, they also pose a problem for privacy. In order to retrieve messages, users must periodically poll the network. The information that the user must give to the network could potentially be used to track that user. However, the movements of the user can also be used to hide the user's location if the protocol for sending and retrieving messages are carefully designed. We have developed a replicated memo system.

10 Anonymizing networks: Reusable anonymous return channels



Philippe Golle, Markus Jakobsson

October 2003 **Proceedings of the 2003 ACM workshop on Privacy in the electronic society V '03**

Publisher: ACM Press

Full text available:  pdf(160.85 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index term](#)

Mix networks are used to deliver messages anonymously to recipients, but do not straightforwardly allow the recipient of an anonymous message to reply to its sender. Yet the ability to reply one more times, and to further reply to replies, is essential to a complete anonymous conversation. We propose a protocol that allows a sender of anonymous messages to establish a *reusable anonymous return channel*. This channel enables any recipient of one of these anonymous messages to send a ...

Keywords: anonymity, mix networks, privacy, return address

11 Routing: ANODR: anonymous on demand routing with untraceable routes for mobile ad-hoc networks



Jiejun Kong, Xiaoyan Hong

June 2003 **Proceedings of the 4th ACM international symposium on Mobile ad hoc networks and computing MobiHoc '03**

Publisher: ACM Press

Full text available:  pdf(236.79 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index term](#)

In hostile environments, the enemy can launch traffic analysis against interceptable routing information embedded in routing messages and data packets. Allowing adversaries to trace network routes and infer the motion pattern of nodes at the end of those routes may pose a serious threat to covert operations. We propose ANODR, an anonymous on-demand routing protocol for mobile ad-hoc networks deployed in hostile environments. We address two closely related problems: For *route anonymity*, AN ...

Keywords: anonymity, broadcast, mobile ad-hoc network, on-demand routing, pseudonymity, trapdoor, untraceability

12 Xor-trees for efficient anonymous multicast and reception



Shlomi Dolev, Rafail Ostrobsky

May 2000 **ACM Transactions on Information and System Security (TISSEC)**, Volume 3 Issue 2

Publisher: ACM Press

Full text available:  pdf(296.45 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index term](#)

We examine the problem of efficient anonymous multicast and reception in general communication networks. We present algorithms that achieve anonymous communication, are protected against analysis, and require $O(1)$ amortized communication complexity on each link and low computational complexity. The algorithms support sender anonymity, receiver(s) anonymity, or sender-receiver anonymity.

Keywords: anonymous communication, anonymous multicast


13 Identification control: Public key distribution through "cryptoIDs"



Trevor Perrin

August 2003 **Proceedings of the 2003 workshop on New security paradigms NSPW '03**

Publisher: ACM Press

Full text available:  pdf(1.51 MB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index term](#)

In this paper, we argue that person-to-person key distribution is best accomplished with a key-distribution approach, instead of PKI: users should distribute public key fingerprints in the same way they distribute phone numbers, postal addresses, and the like. To make this work, fingerprints need to be *small*, so users can handle them easily; *multipurpose*, so only a single fingerprint is needed for each user; and *long-lived*, so fingerprints don't have to be frequently redistributed ...

Keywords: cryptoIDs, fingerprints, key distribution, key management, public key infrastructure

14 Introduction of the asymmetric cryptography in GSM, GPRS, UMTS, and its public key infrastructure integration

Constantinos F. Grecas, Sotirios I. Maniatis, Iakovos S. Venieris
April 2003 **Mobile Networks and Applications**, Volume 8 Issue 2

Publisher: Kluwer Academic Publishers

Full text available:  pdf(107.24 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

The logic ruling the user and network authentication as well as the data ciphering in the GSM architecture is characterized, regarding the transferring of the parameters employed in these processes, by transactions between three nodes of the system, that is the MS, actually the SIM, visited MSC/VLR, and the AuC, which is attached to the HLR in most cases. The GPRS and the U architecture carry the heritage of the GSM's philosophy regarding the user/network authentication the data ciphering ...

Keywords: PKIs, PLMNs, asymmetric cryptography


15 Fine-grained control of security capabilities



Dan Boneh, Xuhua Ding, Gene Tsudik

February 2004 **ACM Transactions on Internet Technology (TOIT)**, Volume 4 Issue 1

Publisher: ACM Press

Full text available:  pdf(128.09 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index term](#)

We present a new approach for fine-grained control over users' security privileges (fast revocation credentials) centered around the concept of an on-line semi-trusted mediator (SEM). The use of in conjunction with a simple threshold variant of the RSA cryptosystem (mediated RSA) offers a number of practical advantages over current revocation techniques. The benefits include simplification of digital signatures, efficient certificate revocation for legacy systems and fast revocation

Keywords: Certificate Revocation, Digital Signatures, Public Key Infrastructure


16 Cryptographic tools: ID-based encryption for complex hierarchies with applications to forward security and broadcast encryption



Danfeng Yao, Nelly Fazio, Yevgeniy Dodis, Anna Lysyanskaya

October 2004 **Proceedings of the 11th ACM conference on Computer and communications security CCS '04**

Publisher: ACM Press

Full text available:  pdf(220.00 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

A forward-secure encryption scheme protects secret keys from exposure by evolving the keys with time. Forward security has several unique requirements in hierarchical identity-based encryption (HIBE) scheme: (1) users join dynamically; (2) encryption is joining-time-oblivious; (3) users evolve secret keys autonomously.

We present a scalable forward-secure HIBE (fs-HIBE) scheme satisfying the above properties. We show how our fs-HIBE scheme can be used to construct a forward-secure ...

Keywords: ID-Based encryption, broadcast encryption, forward security

17 Authentication in distributed systems: theory and practice



Butler Lampson, Martín Abadi, Michael Burrows, Edward Wobber
November 1992 **ACM Transactions on Computer Systems (TOCS)**, Volume 10 Issue 4

Publisher: ACM Press

Full text available: pdf(3.37 MB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index term](#)

We describe a theory of authentication and a system that implements it. Our theory is based on notion of principal and a "speaks for" relation between principals. A simple principal either has a or is a communication channel; a compound principal can express an adopted role or delegated authority. The theory shows how to reason about a principal's authority by deducing the other principals that it can speak for; authenticating a channel is one important application. We ...

Keywords: certification authority, delegation, group, interprocess communication, key distribut loading programs, path name, principal, role, secure channel, speaks for, trusted computing ba:

18 User interface requirements for authentication of communication

Audun Jøsang, Mary Anne Patton

February 2003 **Proceedings of the Fourth Australasian user interface conference on User interfaces 2003 - Volume 18 AUIC '03**

Publisher: Australian Computer Society, Inc.

Full text available: pdf(375.46 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Authentication is a security service that consists of verifying that someone's identity is as claimed. There are a number of challenges to presenting information from the authentication process to user in a way that is meaningful and ensures security. We show examples where authentication requirements are not met, due to user behaviour and properties of existing user interfaces, and suggest some solutions to these problems.

Keywords: authentication, non-repudiation, security, usability, user interface

19 Applied cryptography II: Deniable authentication and key exchange



Mario Di Raimondo, Rosario Gennaro, Hugo Krawczyk

October 2006 **Proceedings of the 13th ACM conference on Computer and communications security CCS '06**

Publisher: ACM Press

Full text available: pdf(266.22 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

We extend the definitional work of Dwork, Naor and Sahai from deniable authentication to denia key-exchange protocols. We then use these definitions to prove the deniability features of SKEM SIGMA, two natural and efficient protocols which serve as basis for the Internet Key Exchange (protocol. SKEME is an encryption-based protocol for which we prove full deniability based on the plaintext awareness of the underlying encryption scheme. Interestingly SKEME's deniability is p the ...

Keywords: authentication, deniability, key exchange

20 Some facets of complexity theory and cryptography: A five-lecture tutorial



Jörg Rothe

December 2002 **ACM Computing Surveys (CSUR)**, Volume 34 Issue 4

Publisher: ACM Press

Full text available: pdf(2.78 MB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index term](#)

In this tutorial, selected topics of cryptology and of computational complexity theory are presen We give a brief overview of the history and the foundations of classical cryptography, and then on to modern public-key cryptography. Particular attention is paid to cryptographic protocols an

problem of constructing key components of protocols such as one-way functions. A function is o if it is easy to compute, but hard to invert. We discuss the notion of one-way functions both ...

Keywords: Complexity theory, interactive proof systems, one-way functions, public-key cryptography, zero-knowledge protocols

Results 1 - 20 of 200

Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2007 ACM, Inc.
[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  [Adobe Acrobat](#)  [QuickTime](#)  [Windows Media Player](#)  [Real Player](#)